Standardization Transparency

An Out of Body Experience[1]

Phillip H. Griffin

Griffin Information Security Consulting, Raleigh, North Carolina, USA

phil@phillipgriffin.com

Abstract. This paper examines the issue of transparency in standards setting organization processes used to select security techniques for standardization. Analysis of data collected from interviews, electronic mail, and other documentation is presented as a narrative in two case studies. A Kaleidoscope conference case study illustrates the positive impacts of open participation on improving transparency through the reduction of bias in the selection process. These impacts include more timely inputs from researchers on emerging technology issues, and greater diversity in the sources of creative new ideas and solutions considered for standardization. Restrictions imposed on the selection process by government control of national body activities are described through a second case study of practice in the United States. Finally, recommendations are proposed on actions standards setting organizations can take to broaden participation in the selection of techniques for standardization and to strengthen communications between standards developers and the research community.

Keywords: openness • security • standardization • transparency

1 Introduction

Transparency is an important issue in the development of security standards for information and communication technology (ICT). Standards development organizations (SDOs) implement processes aimed at enhancing the perception of transparency by standards users and other stakeholders. When SDO transparency is mentioned in research literature, discussion is often confined to processes within a standards development lifecycle that starts with the idea for a new standard. Though the names of lifecycle components vary by SDO, those under SDO control typically begin with creation of a standards project.

The initial selection of techniques for standardization occurs much earlier, before the project is created. A selected technique may stem from an idea, a novel approach, or a perceived need for a standard. Participation in the selection process may be limited to

[1] Paper accepted for presentation at the SSR 2014: Security Standardisation Research Conference, Royal Holloway, University of London, Surrey, UK, http://www.ssr2014.com/

adfa, p. 1, 2014.

a small number of SDO members and not involve most stakeholders. The participants may be biased or serve narrow interests. The selection process may lack transparency, since it occurs on the edge of the standards development lifecycle, before formal SDO approval and project creation. Transparency in the initial selection process is the focus of this paper, and transparency is defined here as the perception of an objective observer that "the process of selecting security techniques for standardization" is "as scientific and unbiased as possible" [1]. Accounts are presented as case studies of the ITU Kaleidoscope conference and United States (US) security standardization practice. These reports are informed by personal experience as a participant in US SDO activities and analysis of data collected from interviews, electronic mail, and other documentation used to examine selection process transparency in global standards setting organizations.

The standardization branch of the International Telecommunication Union (ITU) is the ITU-T. Along with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), these three are considered the global 'de-jure' standards setting bodies [2]. ISO, IEC, and ITU follow "the principle of territorial representation" with their voting members being "national SDO or other national representatives" [3]. There are committees within the global SDO that produce international information security standards (e.g., in ITU-T Study Group 17 Security, ISO/TC68/SC2 Financial Services Security, and ISO/IEC JTC 1/SC 27 IT Security techniques).

Together, ISO, IEC and ITU-T are the "most prominent official international SDO (with national membership)" [3] that produce information security standards. Through its Kaleidoscope conferences, ITU has opened up the standardization selection process to be more inclusive. These conferences attract members of the research and development community that may not participate in national SDO activities. Kaleidoscope provides 'an out-of-body experience' that does not depend on national body approval or processing of proposals considered for standardization.

Through Kaleidoscope conference papers, presentations, discussions, and social events, ITU has found a way to increase the transparency and openness of its standardization selection process. These conferences augment formal ITU standardization practices to include more academic and research institutions and to foster greater input from these important sources of standardization ideas. Section 2 of this paper presents a case study of a paper written by this author that was accepted for the 2013 Kaleidoscope conference. That section describes the impact of the author's paper on information security and data privacy standards.

Governments have an important role to play in national SDO by ensuring transparency and facilitating open participation, and "in stimulating innovation and standardization" in the area of ICT security techniques [4]. Since openness "appears feasible only in a local (maybe national) context", governments should ensure balanced representation in the minority of stakeholders that select technologies for standardization and

that form the delegations attending international standardization committees [3]. From the viewpoint of standards as public goods, governments have a responsibility to promote collaboration among diverse participants having widely different perspectives, expertise, and resources. Governments can act to promote transparency and openness by requiring SDOs to provide "access to standardisation activities without obliging SMEs to become a member of a national standardisation body", "free access or special rates to participate in standardisation activities", and "free access to draft standards" [5].

In the United States, government agencies have taken managerial control over the SDOs that support international standardization of biometrics and IT security techniques. The scope of the primary US security SDO has been changed from one solely devoted to international standards to one whose members also focus on the development and promotion of government sourced national standards. SDO control has been used to ignore technical criticism of agency-sponsored work and to circumvent consensus agreement processes. Section 3 of this paper presents a case study of US standardization practice and its impact on information security standardization.

2 Kaleidoscope Conference Case Study

2.1 Background

The International Telecommunication Union (ITU) was founded in Paris in 1865 to become the first formal standards organization. The ITU was established by the European states as a public-private partnership to create "a forum for the negotiation of standards to ensure network interoperability" [6]. Since its founding, ITU has evolved into a worldwide organization with "a membership of 193 countries and over 700 private-sector entities", including 63 academic and research institutions [2].

The ITU began holding its Kaleidoscope conferences in 2008, with the goal of hosting one conference per year from a different location around the world. An important purpose of these events is to facilitate greater communication between the academic research community and standards developers. To ensure diverse global participation, ITU selects a new conference theme for each event and an academic institution or research organization to serve as conference host [2]. Through the presentation of original, multi-disciplinary papers around a central theme, Kaleidoscope conferences foster dialog between research and practitioner attendees.

Academia is viewed as an important external source of new concepts, technologies, and ideas for ITU-T standardization. Using conference presentations, technical papers, and discussions, the ITU seeks to identify new areas for standardization from outside of its standards development community to support the creation of new or improved ICT products and services. Through its Kaleidoscope conferences, ITU can respond to the increasing "globalization of technology development" and the need for

greater transparency and broader participation in standardization by "opening up of the process to a wider range of actors" [6].

ITU organizes Kaleidoscope conferences in collaboration with the Institute of Electrical and Electronics Engineers (IEEE). ITU publishes accepted academic papers in conference proceedings and ensures their wide dissemination by making them freely available for download from its web site. IEEE lists each paper from the complete proceedings in the IEEE XPlore Digital Library. IEEE also publishes select conference papers that have a high potential impact on standardization in a special standards edition of the IEEE Communications Magazine.

2.2 Openness

The principle of openness in international SDOs is one that has traditionally "put more emphasis on input legitimacy" [3]. To achieve the perception of openness, SDOs establish processes to facilitate stakeholder input as standards are being created, extended, or modified to correct defects. SDO charters, directives, and processes attempt to ensure that "all affected individuals and organizations have the opportunity to get involved in the decision-making process" [3] as standards are being developed. The ITU Kaleidoscope program seeks to apply the principle of openness earlier in the standards development process, to the stage at which security techniques are considered and selected for standardization.

Open participation, inclusiveness, and freedom of discourse are key features of the Kaleidoscope paper acceptance process. Paper submissions may be submitted by anyone from any of the 193 ITU member countries, including students, academics, inventors, and researchers. No topic or content approval by the author's national standards body is required. Authors need not have any experience or prior involvement in standardization activities, and need not be a member of an SDO.

The scope of ITU-T standardization has evolved as telecommunication networks have matured to include standards for multimedia, cloud computing, telebiometrics, information security, and more. Kaleidoscope authors might address any of these areas. Original technical papers can be submitted at no cost, though accepted papers must be presented at the conference by one of the authors to be published. The cost of attending may present a financial obstacle to some authors, and no accommodation is made by ITU for teleconference presentation. There is no academic affiliation requirement, and papers are selected from both academia and industry submissions based strictly on merit. The nationality of the author, the ranking of the author institution or the company size or worth are not considered in the acceptance process.

Submissions are anonymous and peer reviewed against criteria listed in a published rubric using a double-blind process. Unlike many academic conferences, the Kaleidoscope conference uses a scoring rubric to guide authors and reviewers. This rubric is used to evaluate submitted papers based on five criteria: content that demonstrates excellent or novel research, originality, clarity of communication, relevance to the conference objectives, and standards. The standards criterion is weighted higher than the others are. Taken together the criteria call for authors to submit clearly articulated

original research that is relevant to the conference theme and that could have an impact on future ICT standardization.

2.3 Impact on Standardization

From the first six Kaleidoscope conferences held between 2008 and 2014, ITU received important contributions that would influence the course of their standardization efforts. Authors submitted papers to all conferences that identified new areas for ITU-T standardization. Their contributions included a new network architecture, a standards-based service management implementation, and a business model for next generation networks. A recent paper led directly to a new information security standards project for secure messaging to support cryptographic key management techniques.

In the 2008 Innovations in NGN (next generation networks) conference, the best paper described an architecture and business model for an open heterogeneous mobile network. This paper by Murata, Hasegawa, Murakami, Harada, and Kato [7] inspired the creation of a new ITU-T Focus Group on Future Networks (FG FN). Subsequently, future networks became a key theme in ITU-T Study Group 13, underlying their standardization efforts in the areas of cloud computing, NGN, and mobile networks.

The 2009 Innovations for Digital Inclusion conference provided an important model and implementation methodology for quality of service (QoS) management for internet service providers. This award winning contribution was based on extensive review and study of the ITU-T Recommendation E.802 framework described in a paper by Ibarrola, Xiao, Liberal, and Ferro [8]. As participants of an ITU-T Academic Member institution, these authors regularly provide input to the protocols and test specifications standardization work of ITU-T Study Group 11.

The 2013 Building Sustainable Communities conference would provide the first new information security standards project to come from an ITU Kaleidoscope conference presentation. My paper on telebiometric information security and safety management would win an award and reveal security and other defects in several widely used international standards [9] and in the cryptographic messaging used to protect their information. Affected standards included the International Civil Aviation Organization (ICAO) standard for electronic passports, the ISO/IEC 24761 Authentication context for biometrics (ACBio), and the ISO/IEC 19785-4 Common Biometric Exchange Format Framework (CBEFF) – Security block format specifications. Example defects are shown in Fig. 1.

My Kaleidoscope paper noted that while there were several “widely deployed CMS standards”, including the “RSA Public Key Cryptography Standard (PKCS) #7, the Secure Electronic Mail (S/MIME) CMS standard defined by the Internet Engineering Task Force (IETF), and the X9.73 Cryptographic Message Syntax: ASN.1 and XML standard, there was no “normative international CMS standard” that used valid ASN.1 syntax to define its messages [10]. All of the defective security standards

identified in my paper relied on the IETF CMS SignedData type for data integrity and origin authenticity. They all relied on secure messaging that was "based on X.208, the deprecated 1988 version of ASN.1 that was withdrawn as a standard in 2002", and which contained known defects that "were never corrected before it was abandoned" by ISO/IEC and ITU-T [10].

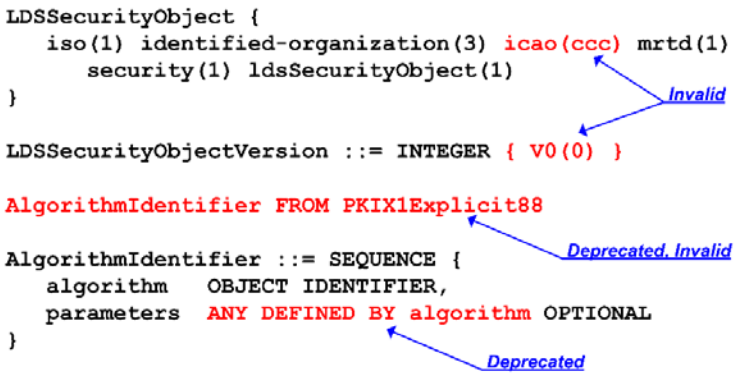

Fig. 1. Invalid and deprecated ICAO schema definitions (Source: IEEE 52.1, p. 188)

Another defect identified in my paper involved the protection provided by "the optional signature block defined in the ISO/IEC 19785 CBEFF standard" [10]. A cryptographic message wrapper that encapsulates the entire template provides stronger protection of biometric templates in some environments than using the optional CBEFF security block. Using a message wrapper approach "allows a trivial attack on reference templates to be detected using signature verification" [10]. As described in Fig. 2, when used in "environments in which the optional signature block is not required to be present, it is possible for a low skill attacker to remove the entire signature block to thwart the signature safeguard's effectiveness" [10].

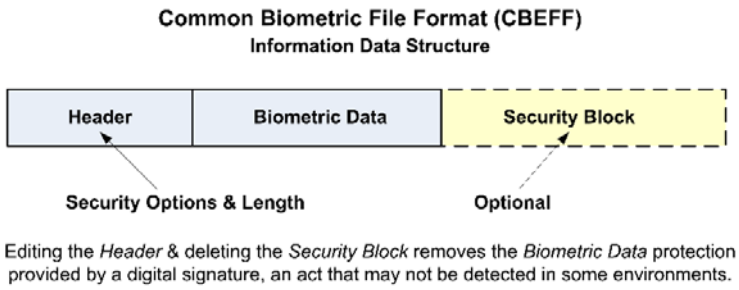

Fig. 2. Security vulnerability (Source: IEEE 52.1, p. 189)

My Kaleidoscope paper proposed four areas for standardization. One information security proposal called for the creation of an international Cryptographic Message Syntax (CMS) standard containing correct messaging syntax and based on the current ASN.1 standards. A new CMS standard could be used to correct defects identified in the ICAO, ACBio, and CBEFF standards. A second proposal called for the standardization of a new SigncryptedData CMS message type. Two biometric information management and security proposals called for the creation of a standard event journal and security alert system for logging distributed biometric system security and safety events, and for the creation of a telebiometric system heartbeat message that could support optional inclusion of digitally signed or signcrypted ACBio system security verification reports [9].

2.4 Security Standards Proposals

During the 2013 conference in Kyoto, the Kaleidoscope Secretariat and her staff informed me that they had submitted my conference paper and presentation deck to the delegates of the ongoing ITU-T Study Group 17 Security meeting. A staff member arranged for me to make a presentation to the Question 9 (telebiometrics) standardization delegates meeting that week in Geneva. A member of the ITU Telecommunications Standards Bureau and the conference hosts arranged to provide an office next to the conference auditorium, a laptop, and a headset for the remote presentation of my proposals for new standardization.

The presentation was well received and followed by a brief question and answer session. However, neither of the biometric security management proposals described in the presentation would result in new standardization projects. The author would later discuss these proposals with a US delegate to SG17 who had not attended the Question 9 meeting in Geneva. After being thanked for presenting new standardization proposals to the committee, the delegate advised the author that the National Institute of Standards and Technology (NIST) was opposed to any biometrics standardization work being performed outside of the ISO/IEC JTC 1/SC 37 Biometrics group. The delegate noted that it would not be possible to propose new biometric standards development work from the US without NIST approval, and that the Kaleidoscope biometric security management proposals would not be put forward for consideration as new work items. No documentation was offered as evidence by the delegate that their remarks were an official US government position.

My 2013 Kaleidoscope paper and presentation slide deck were also provided to Study Group 17 Question 11 (Specification and Implementation Languages) for review. The two secure message proposals in the paper were viewed favorably, and the Rapporteur to the Study Group 17 plenary from France submitted a new work item proposal. The proposal was approved, and a project was started to create an international CMS standard that would correct and extend the defective Internet Engineering Task Force (IETF) CMS standard. The new CMS project would include a Signcrypted data type based on the ISO/IEC 29150 Signcryption security standard. No US approval was required to submit or approve the CMS new work item proposal.

3 US Practice Case Study

3.1 Government Roles

The American National Standards Institute (ANSI) is the US national body member of two of the three global SDOs responsible for information security standardization: ISO and IEC. The third SDO is ITU-T, which produces some security standards jointly with ISO and IEC, and whose US member is the US Department of State. ANSI establishes "the standards setting process that US national SDOs need to implement" to ensure their operations are based on "attributes like openness and transparency" [11]. There are over 200 ANSI-accredited SDOs in the US system, each typically associated with a single industry sector. NIST plays a special role in US standardization.

NIST "co-ordinates standards policy among the federal agencies", who are "encouraged to actively contribute to standards setting and to standards policy" as required by the National Technology Transfer and Advancement Act (NTTAA) [11]. Ideally, the role of NIST would be indirect, and as suggested by Sherif and Seo, limited to "promoting an environment in which firms can be innovative" and "promoting quality and performance standards with a global focus" [4]. However, NIST does not perform a limited, indirect role in US information security standardization. NIST contributes significant technical expertise to the development of international security standards. NIST also contributes the time of employees who have served as talented technical editors (i.e., ISO/IEC 29150, ISO/IEC 19790, etc.). However, a primary focus of NIST has been on national standards that serve government agency needs rather than on global standards that serve wider US interests [12].

Jakobs recognizes that the US government plays important coordination and promotional roles in standardization. He notes that with respect to technical details, "the US administration does not intervene in the process" of standardization, "nor does it mandate any standards" [11]. Rather, proposals developed by US SDOs result in voluntary, consensus standards. However, for information security standards there have been notable exceptions to this view.

These exceptions have resulted in defects remaining uncorrected for years in some standards. This was noted at Kaleidoscope 2013 in my presentation describing CBEFF defects and the defective information exchange syntax used in a widely referenced IETF cryptographic message standard. Government restrictions on the development of new standards are illustrated in the treatment of proposals for telebiometric security management standards described above. In the case of the NIST Role Based Access Control (RBAC) standard, there has been direct government intervention in the technical details of a security standard and in the consensus standards process.

3.2 Role Based Access Control

The NIST timeline for its RBAC standard starts in 2004. In that year, ANSI International Committee for Information Technology Standards (INCITS) adopted the

"RBAC proposal as an industry consensus standard" [13]. Consensus agreement on the proposal was reached by the INCITS Executive Board, but it was never reached in the committee assigned by INCITS to review and comment on the technical details of the proposal. While under review by the T4 IT Security Techniques committee, the RBAC proposal failed to pass successive ballots. These failures were due to technical defects that subsequent research described as "limitations, design flaws, and technical errors" [14].

The authors of the RBAC proposal never addressed editorial and technical defects cited in the ballot comments of T4 members. Following a second failed ballot, T4 invited the authors to discuss how the concerns of the committee might be resolved, but received no response. Instead, NIST intervened directly in the standardization process. Using its standing as a member of the INCITS Executive Board, NIST appealed directly to the board for approval. Ignoring the sustained technical concerns raised by T4 members, the INCITS board approved the RBAC proposal as ANSI INCITS 359-2004, despite "a number of spelling and technical errors in the standard" [14].

Hoel argues that the role of government in standardization should be minimal. If government is to support technology innovation, direct government control is not needed, but instead, "initiatives to support consensus processes, in which governments do not have the final word regarding technical details" [15]. In the case of RBAC, NIST bypassed the consensus building process, and failed to reach agreement with fellow T4 members or to respond to their criticism of its work.

Following the negative committee response to its RBAC proposal, the role of NIST in the standardization of security techniques changed. NIST went from being an important technical contributor to assuming a more direct and controlling managerial role over the US SDO for information security. In 2005, NIST proposed that the INCITS Executive Board create a new security committee, one that could focus on the development of US national standards in its program of work [12], standards in which the T4 committee had expressed no interest. The INCITS board approved the proposal and created the CS1 Cyber Security committee. NIST has chaired CS1 since its inception, giving it greater control over US contributions to international security standardization.

In its recommendation to create INCITS CS1, NIST proposed that the T4 committee be stripped of most of its Technical Advisory Group (TAG) responsibilities in ISO/IEC JTC 1/SC27 IT Security techniques. Despite the growing global adoption of the ISO/IEC 17799 Code of practice for information security management [16], the NIST proposal asserted that there was not "wide consensus on best practices for information security management" and proposed development of a US national standard for "Risk Based Information Security Management" based on work "in progress at NIST" [12]. NIST proposed further development of national standards, such as extension of the RBAC standard and development of an IT security metrics standard with no indication given that these would be proposed for international standardization. This direct intervention in US security SDO practices by NIST changed the di-

rection of US efforts from a focus on international information security standards to a focus on competing national alternatives.

3.3 Cryptographic Message Syntax

RSA Data Security first proposed the Secure/Multipurpose Internet Mail Extensions (S/MIME) for IETF standardization in the mid-1990s. The RSA proposal was based on their proprietary secure messaging standard, RSA Public Key Cryptography Standard 7 (PKCS #7) Cryptographic Message Syntax (CMS). NIST has a long history of involvement in the development of IETF CMS and in its promotion.

The 2002 NIST Special Publication (SP) 800-49 Federal S/MIME Client Profile recommends a version of IETF CMS whose message schema is based on the 1988 and 1990 Abstract Syntax Notation One (ASN.1) standards, X.208 and X.209 [17]. Both X.208 and X.209 were withdrawn as international standards that same year, 2002, due to well-known deficiencies and documented defects [18]. Their withdrawal followed several years in which they had been formally deprecated, and users in IETF and elsewhere encouraged to migrate to the current ASN.1 standards.

X.208 and X.209 were replaced and superseded by the X.680 and X.690 series of ASN.1 standards in 2002. These replacements corrected all known defects in the withdrawn versions, but these defects were never removed from X.208 and X.209. Efficient national language support in the current ASN.1 standards was never added to X.208. The XML Encoding Rules (XER), and the Distinguished Encoding Rules (DER) that provide the unambiguous data representations required by CMS and other cryptographic protocols were never defined for use with the X.208 syntax. Reliance on invalid and deprecated cryptographic message schema for data security in the AC-Bio, CBEFF, and ICAO standards does not enhance their ability to provide information assurance and security.

Recently, reference to IETF 3852 CMS began to appear in several important international biometrics and information security standards, despite its continued reliance on withdrawn standards to define its secure information exchange messages. Affected standards that depend on CMS for data security include ICAO electronic passports, ISO/IEC 24761 biometric security, ISO/IEC 19785-4 biometrics, and the ANSI/NIST-ITL biometric information exchange standard widely used by law enforcement and defense agencies. The design of the optional US National Security Agency (NSA) Type-98 information assurance record in the ITL standard is based on the same approach described in Fig. 2.

A paper presented at the 2013 ITU Kaleidoscope conference in Kyoto described these issues and recommended corrections [9]. The presentation proposed that ITU-T create a new international CMS standard that would correctly use the current ASN.1 schema definition standards. Once completed, a new corrected CMS standard could be referenced in other international security standards. Like most ITU-T standards it would be freely available to SDOs and implementers. Following approval of a new CMS project by Study Group 17, work began in January 2014 on a joint ISO/IEC 24824-4 standard and ITU-T 'x.CMS' recommendation.

The selection of CMS security techniques for standardization did not require the approval of the national body of the proposer, or on national body procedural support. The proposal did not depend on membership in a national body SDO. ITU Kaleidoscope conferences provide a venue that allows proposals to be presented, discussed, and evaluated strictly on their technical merits. These conferences establish an important new open and transparent process for the initial selection of security techniques for standardization that can circumvent restrictions that may be imposed by government controlled SDO.

4 Conclusion and Recommendations

From its roots as the first international standards organization, ITU has again shown the way forward for global SDO that strive to remain relevant in an increasingly interdependent world of rapidly changing technology. ITU Kaleidoscope conferences foster greater openness and transparency in the initial selection of security techniques for international standardization. Kaleidoscope conferences invite new proposals for standardization from the broad community of academic and research institutions. Participation is not limited to national SDO members, but open to all standards stakeholders, to everyone who lives in an ITU member country.

Kaleidoscope conferences are hosted by academic and research institutions at different locations around the world. These events bring standards developers together with inventors and researchers who are closest to new and emerging technologies that may be appropriate for standardization. The Kaleidoscope proposal process shortens the

gap between the discovery of innovative solutions and their standardization, and can circumvent restrictions imposed by government controlled national SDO.

ITU could improve their conferences by allowing authors to present their work remotely by teleconference or videoconference. Author presentations could also be recorded and made freely available by ITU in audio or video format, as is presently the case for USENIX security conferences. Recorded presentations could provide an additional educational benefit and enhance the ability of the conference to foster the free exchange of research information.

The US economy is diverse and immense. The broad interests of US standards stakeholders cannot be served by a single government agency alone. The government should not have the final say on the technical details of any standard, especially security standards such as RBAC or CMS. NIST should play only an indirect role in international standardization, a role that facilitates open, transparent processes that benefit all standards stakeholders.

NIST should not exert managerial control over SDO activities or use SDO management boards to quash technical criticism of their work. They should limit their involvement to promoting standards adoption and use, providing contributions of technical expertise, and promoting broad and inclusive participation. In an increasingly global economy, NIST would better serve the interests of US citizens and businesses by promoting the development and adoption of international standards, rather than promoting their own information security and information security management work as sources for national standards alternatives.

Recently, security techniques proposed at a Kaleidoscope academic conference resulted in creation of a new international standardization project in ITU. All of the global security SDOs could benefit from the closer ties to researchers afforded by the ITU model. The SC 27 IT Security techniques and TC68/SC2 Financial Services Security groups should provide a means for academic papers and conference presentations to inform their information security standardization selection processes. They should encourage greater openness through wider participation in the development of new standards by academic and research institutions.

The ITU Kaleidoscope conference serves as a model to be replicated by others. Conferences with a focus on information security techniques that can provide new inputs for international security standardization should be sponsored by security standards setting bodies. Sponsored conferences should be attended by SDO representatives who can transform proposals into actions, such as the creation of study groups and new work item proposals. Examples of promising conferences to be considered include the new 2014 Security Standardization Research (SSR) conference in the United Kingdom and the 2014 International Conference on Smart Computing in Hong Kong.

References

1. SSR 2014: Security Standardisation Research, http://www.ssr2014.com/
2. International Telecommunication Union, http://www.itu.int
3. Werle, R., Iversen, E.: Promoting legitimacy in technical standardization. In: Science, Technology & Innovation Studies, vol. 2. 2006
4. Sherif, M. H., Seo, D.: Government role in information and communications technology innovations. In Innovations for Digital Inclusions. ITU-T Kaleidoscope*:* (pp. 1-5). IEEE. 2009.
5. Regulation of the European Parliament and Council, (EU) No 1025/2012, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025
6. Graham, I.: Reflexive Standardization of Network Technology. In: Proceedings of the ITU Kaleidoscope Academic Conference, pp. 83–88. 2011
7. Murata, Y., Hasegawa, M., Murakami, H., Harada, H., and Kato, S.: The architecture and a business model for the open heterogeneous mobile network. In Proceedings of the 2008 ITU Kaleidoscope Academic Conference: Innovations in NGN, pp. 143-150. 2008, http://www.itu.int/pub/T-PROC-KALEI-2008/en
8. Ibarrola, E., Xiao, J., Liberal, F., and Ferro, A.: Quality of Service management for ISP: A model and implementation methodology based on ITU-T Rec. E.802 framework. In Proceedings of the 2009 ITU Kaleidoscope Academic Conference: Innovations for Digital Inclusion, pp. 35-42. 2009, http://www.itu.int/pub/T-PROC-KALEI-2009
9. Griffin, P: Telebiometric Security and Safety Management. In Proceeding of the 2013 ITU Kaleidoscope Academic Conference: Building sustainable communities, pp. 127-134. 2013, http://www.itu.int/pub/T-PROC-KALEI-2013
10. Griffin, P: Telebiometric Security and Safety Management. *Communications Magazine, IEEE*, 52.1, 186-192, 2014.
11. Jakobs, K.: ICT Standardisation in China, the EU, and the US. In: Innovations for Digital Inclusions, 2009. K-IDI 2009. ITU-T Kaleidoscope: pp. 1-6. IEEE, 2009.
12. INCITS Proposal to create new security technical committee CS1, in050057, 2005, http://csrc.nist.gov/groups/SNS/rbac/documents/in050057.pdf
13. National Institute of Standards and Technology - Computer Security Resource Center, http://csrc.nist.gov/groups/SNS/rbac/faq.html#timeline
14. Li, N., Byun, J., Bertino, E.: A Critique of the ANSI Standard on Role Based Access Control. *Security & Privacy, IEEE*, *5*(6), 41-49. 2007.
15. Hoel, T.: Paradoxes in LET standardisation–towards an improved process. In: Proceedings of the 21st International Conference on Computers in Education. Indonesia: Asia-Pacific Society for Computers in Education. 2013.
16. Backhouse, J., Hsu, C., and Silva, L.: Circuits of power in creating de jure standards: shaping an international information systems security standard. In: MIS quarterly, vol. 30, 2006, pp. 413-438.
17. National Institute of Standards and Technology SP 800-49 Federal S/MIME V3 Client Profile, http://csrc.nist.gov/publications/nistpubs/
18. ITU-T Recommendation X.208, https://www.itu.int/rec/T-REC-X.208/en